УДК 004.056.55

Красиленко В. Г., канд. техн. наук., старш. наук. співроб., доцент,
Нікітович Д. В.
Вінницький національний технічний університет

ПРОТОКОЛИ УЗГОДЖЕННЯ СЕКРЕТНИХ КЛЮЧІВ У ВИГЛЯДІ МАТРИЧНИХ ПЕРЕСТАНОВОК ЗНАЧНОЇ РОЗМІРНОСТІ ДЛЯ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ

Вступ. Узагальнення відомих криптосистем з форматами даних скалярного типу на випадки матрично-тензорних форматів, поява та дослідження нового класу криптосистем матричного типу (КМТ) [1-4] на основі їх матрично-алгебраїчних моделей (МАМ) криптографічних перетворень (КП) 2D(3D) - масивів, зображень (З), які мають ряд суттєвих переваг, сприяла інтенсифікації досліджень КМТ, МАМ та демонстрації цілої низки нових їх покращень та застосувань [5-10]. Узагальнені МАМ, матричні афінні та афінно-перестановочні шифри (МАПШ), їх модифікації досліджувались та використовувались при створенні сліпих та інших покращених цифрових підписів у [11-15]. МАМ при їх апаратних реалізаціях легше відображаються на матричні процесори, мають розширені функціональні можливості, покращену крипто-стійкість, дозволяють перевіряти цілісність криптограм чорно-білих, кольорових зображень і наявність у них перекручувань [5,7], створювати блокові [6], параметричні [8], багатосторінкові [9] моделі з їх значною стійкістю [10]. Для КП у матричних моделях перестановок (ММ_П), з їх базовими процедурами множення матриць та деякими іншими по-елементними операціями за модулем над матрицями, матриці байтів, утворених з ряд-ків, колонок, векторів, що в унітарних чи інших кодах відображають символи, коди, байти, необхідно множити на матриці перестановок (МП). Процедури переставляння бітів, байтів чи їх груп є найбільш поширеними та обов'язковими практично для всіх відомих та новостворюваних алгоритмів та шифрів. Для збільшення ентропії криптограм З при їх КП на основі ММ_П та зміни їх гістограм необхідні декомпозиція R,G,B складових і їх бітових зрізів та декілька матричних ключів (МК) типу МП [3-5]. Низка таких псевдовипадкових (поточних, покрокових, по-фреймових) МК, які б відповідали вимогам, швидко генерувались, потрібна і для маскування, КП відео-файлів чи потоку блоків з файлів, зображень при їх значних розмірах. Постановка задачі. Таким чином, для МАМ є необхідність формування низки МП, які б задовольняли ряду вимог, з головного МК. Оскільки питання узгодження головного МК загального виду, але не послідовності МП розглядались в [16,17], а методи генерування потоку МК перестановок з головного МК частково розглядались в [18], але тільки для бітових МП невеликих розмірів (256*256), то метою роботи є спроба запропонувати та дослідити протокол узгодження секретного (головного) МК у вигляді МП значної розмірності, тобто ГМП, удосконалити та адаптувати вид, структуру ГМП такої чи ще значнішої розмірності до формату З і до швидких апаратних рішень, промоделювати цей протокол та процес формування потоку МП з такої ГМП для МАМ КП у системах МТ.

Виклад основного матеріалу та результатів дослідження. Огляд МТ шифрів, особливо багатофункціональних параметричних блочних [4], їх аналіз показують, що доцільно використовувати для досягнення мети ізоморфність різних представлень перестановок (матриць чи векторів), що виступають у ролі головного ключа (ГК) та по-блокових чи покрокових, раундових МК типу МП, тобто під-ключів (ПК), що являють собою матриці перестановок P (її степені !) чи ізоморфні їм вектори. З робіт [6,8,9] відомо, що при КП на основі МАПШ, ВАПШ криптограми для деяких видів текстово-графічних документів (ТГД) і З, особливо для поблочних МАМ, при використанні одного ПК для всіх блоків є недостатніми по стійкості, та попри це низка ПК, що створюються з ГК, вирішує цю проблему. А тому важливим є аспект узгодження секретного ГК типу МП значної розмірності. Розглянемо ситуацію, коли для КП блоків довжиною 256*256 байтів, що представлені у вигляді матриці чорно-білого зображення необхідно переставити всі байти у відповідності до МП. В цьому випадку МП в загально прийнятому вигляді повинна бути квадратною з N*N елементами («0» чи «1»), де $N=2^{16}$. Потужність множини можливих таких МП, тобто їх кількість оцінюється, як N!, що дає для цього N колосальні значення. Але кожну адресу байту блоку можна представити і за допомогою двох байтів, що вказують дві координати (рядок та стовпчик) блоку. Це дає нам можливість двома блоками (256*256 елементів) байтів представляти любу перестановку, ставлячи в кожній однаковій адресі цих блоків відповідну старшому байту (в першому блоці) та молодшому байту (в другому блоці) координати нової адреси вибраного для перестановки байту. Вигляд програмного модуля у Mathcad для генерування базового (головного) МК (МП) та вигляд його складових KeyA та KeyB у форматі двох чорно-білих зображень показано на рис.1. Отже, любу МП можна однозначно відобразити двома матрицями розміром 256*256, елементи яких приймають значення з діапазону 0-255, з тією особливістю, що кожна з 256 їх градацій інтенсивності в кожній з цих двох матриць (З) повторюється рівно по 256 раз. Гістограми складових KeyA та KeyB МП зображені на рис.2 та мають вигляд горизонтальних ліній, як і очікувалось. Відмітимо, що таке ізоморфне у вигляді двох зображень представлення МП дає нам можливість використати ці складові KeyA та KeyB у якості двох сек-ретних МК загального типу, наприклад, як адитивний та мультиплікативний ключі у МАПШ чи іншій МАМ. Про це свідчать результати моделювання КП зображення (Im) МАПШ за допомогою пропонованої МП та її складових, як ключів, що показані на рис. 3 з матрицями явного З (Im), проміжних, його криптограм (Cmap) та перевірних З [19]. А гістограми явного З, його криптограм після кожного КП афінними складовими цієї МП зображені на рис.2.

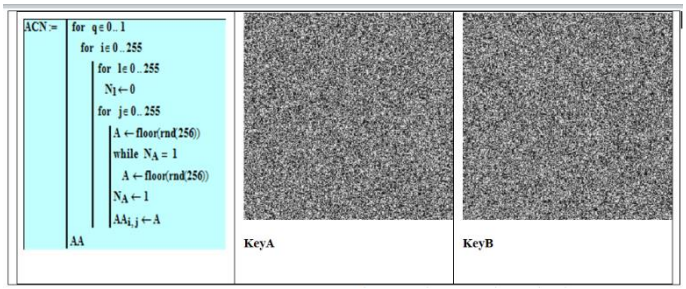

Рис. 1. Програмний модуль для генерування базового (головного) МК (МП) та вигляд складових KeyA та KeyB у форматі двох чорно-білих зображень (Вікно Mathcad).

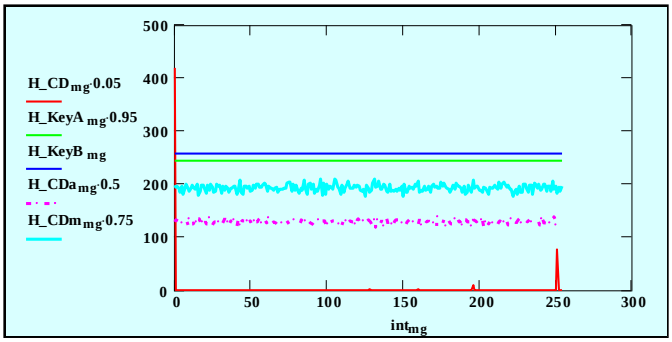

Рис. 2. Гістограми H_KeyA та H_KeyB відповідно складових KeyA та KeyB МП, гістограма H_CD криптограми явного З (співпадає з гістограмою З), відповідні гістограми H_CDa та H_CDm криптограм після адитивної та мультиплікативної афінних КП З за допомогою тих же KeyA та KeyB (Вікно Mathcad).

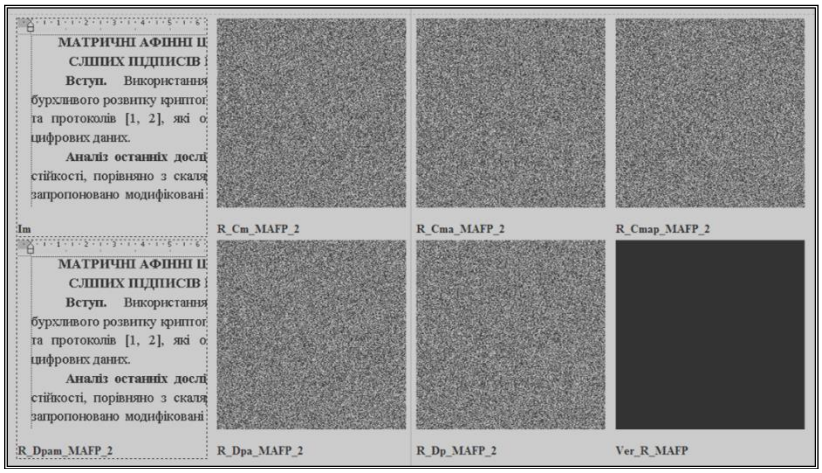

Рис. 3. Результати моделювання МАПШ на основі МП та її складових, як адитивного та мультиплікативного МК. Верхній ряд, зліва направо: явне, після перетворень, криптограма після МАПШ; Нижній ряд: відновлене, проміжні та різницеве (праворуч) зображення ТГД.

Ці модельні експерименти підтвердили, що КП МАПШ наявними 2-ма складовими МП дають якісні криптограми CD_ImAa та CD_ImAm, гістограми яких H_CDa та H_CDm настільки близькі до рівномірного закону розподілу, що навіть для З (Im) з ентропією 0,738 ентропія криптограм відрізняється від теоретично максимальної (8 біт) всього на долі відсотка, збільшуючись аж до 7,99. Результати моделювання МАПШ та багатокрокових МАПШ для різних випадків, коли спочатку виконуються складові афінних перетворень і у іншій послідовнос-ті та різними чи одним МК від МП, а потім перестановка за допомогою МП, чи навпаки, також засвідчили подібні якісні КП при застосуванні пропонованих представлень МП. Але для всіх модифікацій МАМ при таких МП, потужність множини яких оцінюється значною величиною N!=(256*256)!, є надважливим питання узгодження сесійної секретної ГМП. А тому, узагальнюючи наш підхід, можна стверджувати, що для синтезу ГМП зі значно більшою розмірністю останні можна також однозначно представити за допомогою 3, 4 і т.д. зображень-матриць чи блоків з байтів, аналогічних вищевказаним складовим KeyA та KeyB.

Розглянемо сутність самого протоколу узгодження ГМП сторонами. Нехай є сторони: *x* (Alisa) та *y* (Bob). Допустимо, що відома одна МП з множини допустимих у вигляді складових KeyA та KeyB, що показана на рис. 4. Крім того, завжди існує МП зворотної перестановки, що для вибраного представлення має вигляд 2-х З KeyAO та KeyBO. Кожна з сторін на першому кроці підносить ізоморфно ГМП у вибрану ними свою

секретну степінь (у нас 11 та 17 для прикладу !), пересилає нову МП іншій стороні та на другому кроці сторону отримані нові МП аналогічно підносять їх у ті ж свої випадкові секретні степені. Тут аналогія з протоколом Діффі-Хелмана. На рис. 5-8 показані результати моделювання цих двох кроків протоколу узгодження секретного МК у Mathcad, а на рис.9-10 вигляд отриманих проміжних та результативної секторної ГМП у ізоморфному представленні З. Сторони не знають степені іншої сторони, але отримані ними МП є ідентичними, що видно з рис. 10.

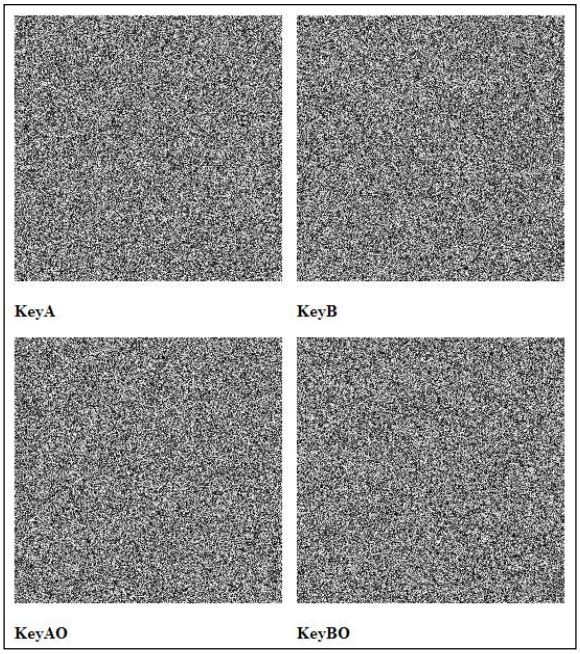

Рис. 4. Вигляд (2D) відомих генерованих МП: вгорі (пряма), внизу (зворотна) перестановки.

Таким чином піднесення МП (N*N бінарних, де $N=2^{16}!$) еквівалент-но замінюється швидкими перестановками, які до того ж можуть бути ще більш прискореними при значних степенях за рахунок використання деякого базового набору фіксованих (фіксовані степені ГМП) та специфічної їх послідовності, що дає досягнення суттєвих переваг за рахунок прискорень обчислення степенів ГМП, простоти можливих реалізацій і зменшення затрат.

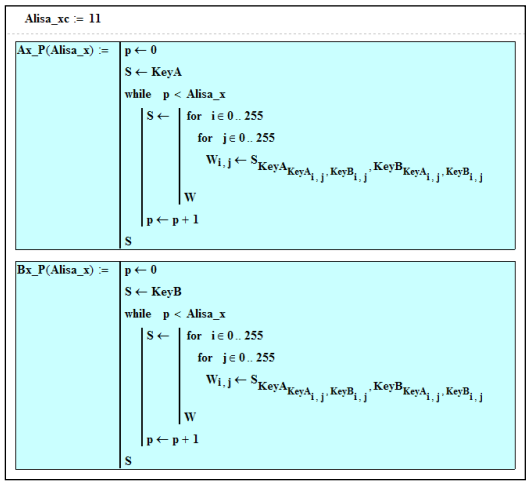

Рис. 5. Програмні модулі (копії з Mathcad), що відображають процедуру ітераційних перестановок в МП, ізоморфних піднесенню матриці перестановки у потрібну степінь (11 !) стороною *x* (Alisa).

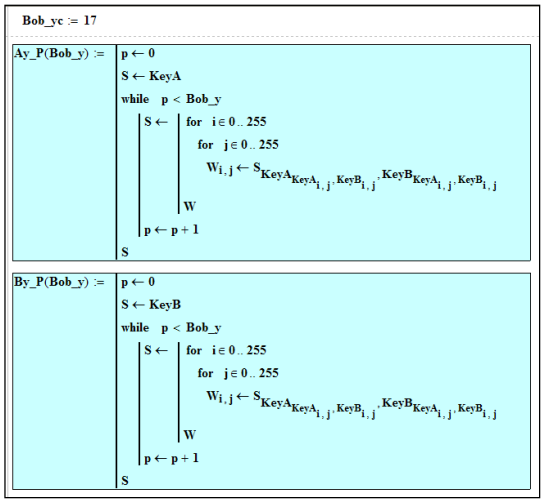

Рис. 6. Програмні модулі (копії з Mathcad), що відображають процедуру ітераційних перестановок в МП, ізоморфних піднесенню матриці перестановки у потрібну степінь (17 !) стороною *y* (Bob).

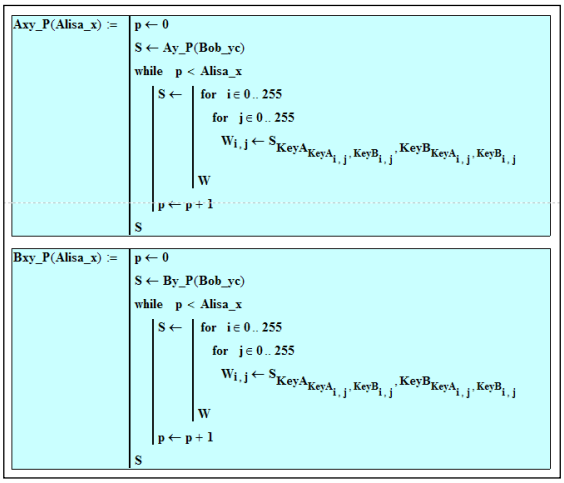

Рис. 7. Програмні модулі (копії з Mathcad), що відображають процедуру ітераційних перестановок в отриманій від *y* новій МП, ізоморфних піднесенню у потрібну степінь (11 !) стороною *x* (Alisa).

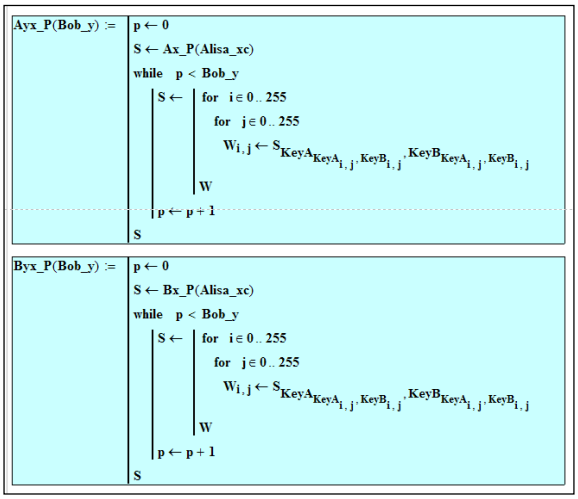

Рис. 8. Програмні модулі (копії з Mathcad), що відображають процедуру ітераційних перестановок в отриманій від *x* новій МП, ізоморфних піднесенню у потрібну степінь (17 !) стороною *y* (Bob).

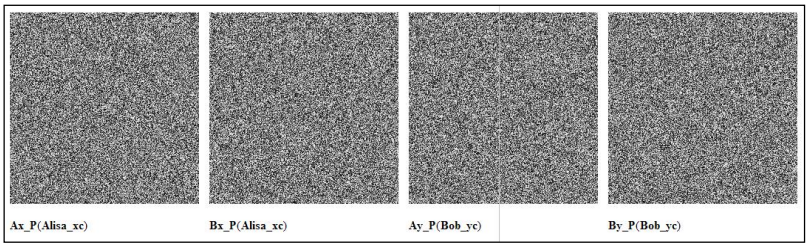

Рис. 9. Отримані сторонами нові МП (кожна у вигляді їх двох складових) після першого кроку протоколу, ті що пересилаються іншій стороні.

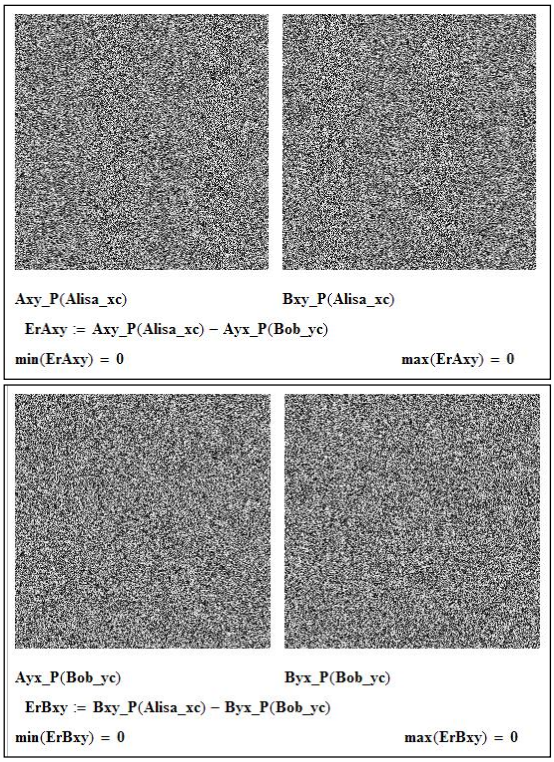

Рис. 10. Отримані сторонами ідентичні нові МП (кожна у вигляді їх двох складових) після другого кроку протоколу, тобто секретна МП.

Використовуючи розроблені функціональні параметричні моделі КП за допомогою узгодженого пропонованим протоколом секретного МК, що показані вище, було виконано перевірку правильного до вимог їх синтезу та адекватності моделей шляхом прямого та зворотного КП 3, що було показано на рис. 1-3. Отримані моделюванням у Mathcad результати підтверджують правильність протоколу, а аналіз стійкості, що буде представлений детальніше у доповіді, показує неможливість здійснення атак внаслідок величезної множини можливих МП.

Висновки. Запропоновано протокол узгодження секретного ключа у вигляді ізоморфних представлень МП значних розмірностей, виконано модельні експерименти, що підтвердили адекватність функціонування моделей та пропонованих протоколу і методів генерування МП, їх переваги. Моделі прості, зручні, адаптуються для різноформатних та кольорових зображень, реалізуються матричними процесорами, мають високі ефективність, стійкість, швидкодію.

Список літературних джерел

1. Красиленко В.Г. Моделювання матричних алгоритмів криптографічного захисту / В.Г. Красиленко, Ю.А. Флавицька // Вісн. НУ "Львів. політехніка".- 2009. - № 658. - С. 59-63.

2. Красиленко В. Г. Матричні афінно-перестановочні алгоритми для шифрування та дешифрування зображень / В. Г. Красиленко, С. К. Грабовляк // Системи обробки інформації. - 2012. - Вип. 3(2). - С. 53-61. - Режим доступу: http://nbuv.gov.ua/UJRN/soi_2012_2_3_15

3. Красиленко В.Г. Криптографічні перетворення зображень на основі матричних моделей перестановок з матрично-бітовозрізовою декомпозицією та їх моделювання / В. Г. Красиленко, В. М. Дубчак // Вісник Хмельн. НУ. Технічні науки. - 2014. - № 1. - С. 74-79.

4. Красиленко В.Г. Моделювання криптографічних перетворень кольорових зображень на основі матричних моделей перестановок зі спектральною та бітово-зрізовою декомпозиціями / В.Г. Красиленко, Д.В. Нікітович // Комп'ютерно-інтегровані технології: освіта, наука, виробництво : наук. журн. – Луцьк:

Видавництво Луц. нац. техн. ун-т., - 2016. - № 23. - С. 31-36. – Режим доступу: http://ki.lutsk-ntu.com.ua/node/132/section/9 .

5. Красиленко В.Г. Моделювання та дослідження криптографічних перетворень зображень на основі їхньої матрично-бітовозрізової декомпозиції та матричних моделей перестановок з верифікацією цілісності / В.Г. Красиленко, Д.В. Нікітович // Електроніка та інформаційні технології. – Львів: ЛНУ імені Івана Франка, 2016. – Вип. 6. – С 111-127. – Режим доступу: http://elit.lnu.edu.ua/pdf/6_12.pdf

6. Красиленко В.Г. Моделі блокових матричних афінно-перестановочних шифрів (МАПШ) для криптографічних перетворень та їх дослідження / В.Г. Красиленко, Д.В. Нікітович // 72 НТК: матеріали конференції (13-15 грудня 2017 р.). – Одеса: ОНАЗ ім. О.С. Попова, 2017. – Частина 1. – С.117-122.

7. Красиленко, В.Г. Моделювання матричних афінних алгоритмів для шифрування кольорових зображень / В. Г. Красиленко, К. В. Огородник, Ю.А. Флавицька // Комп'ютерні технології: наука і освіта: тези доповідей V Всеукр. НПК– К., 2010. – С.120-124.

8. Красиленко В.Г. Багатофункціональні параметричні матрично-алгебраїчні моделі (МАМ) криптографічних перетворень (КП) з операціями за модулем та їх моделювання. / В.Г. Красиленко, Д.В. Нікітович. // 72 НПК: матеріали конференції (13-15 грудня 2017 року). – Одеса: ОНАЗ ім. О.С. Попова, 2017. – Частина 1. – С.123-128.

9. Красиленко В.Г. Моделювання сторінкових криптографічних перетворень масивів кольорових зображень на основі матричних моделей та перестановок / В.Г. Красиленко, Д.В. Нікітович // «Інформаційно-комп'ютерні технології – 2018»: Збірник тез доповідей IX Міжнародної НТК, 20-21 квітня 2018 року. – Житомир: Вид. О. О. Євенок, 2018. – С. 73-77.

10. Красиленко В.Г. Дослідження покращеного багатокрокового 2D RSA шифру та його гістограмно-ентропійних характеристик / В.Г. Красиленко, Д.В. Нікітович // «Інформаційна безпека та комп'ютерні технології»: Збірник тез доповідей III Міжнародної НПК, 19-20 квітня 2018 року. – Кропивницький: ЦНТУ, 2018. – С. 78-82. Режим доступу: http://it-kntu.kr.ua/wp-content/uploads/2015/01/Zbirnyk-tez-InfoSecCompTech-2018.pdf

11. Красиленко В.Г. Матричні афінні шифри для створення цифрових сліпих підписів на текстографічні документи / В.Г. Красиленко, С.К. Грабовляк // Системи обробки інформації. – Х.: ХУПС, 2011. – Вип. 7(97). – С. 60 – 63.

12. Красиленко В.Г. Демонстрація процесів створення сліпих електронних цифрових підписів на текстографічну документацію на основі моделей матричного типу / В.Г. Красиленко, Р.О. Яцковська, Ю.М. Тріфонова, // Системи обробки інформації. – 2013. – Вип. 3(110). – Т. 2. – С. 18 – 22.

13. Красиленко В.Г. Вдосконалення та моделювання електронних цифрових підписів матричного типу для текстографічних документів / В.Г. Красиленко, Д.В. Нікітович // Матеріали VI міжнародної науково-практичної конференції «Інформаційні управляючі системи та технології» (ІУСТ-Одеса-2017), Одеський національний морський університет, 20-22 вересня 2017р. – Одеса: «ВидавІнформ НУ «ОМА», 2017. - С. 312 -318.

14. Красиленко В.Г. Моделювання покращених сліпих електронних цифрових підписів 2D типу / В.Г. Красиленко, Д.В. Нікітович // «Інформаційно-комп'ютерні технології – 2018»: Збірник тез доповідей IX Міжнародної науково-технічної конференції, 20-21 квітня 2018 року. – Житомир: Вид. О. О. Євенок, 2018. – С. 78-82.

15. Красиленко В.Г. Моделювання покращених багатокрокових 2D RSA алгоритмів для криптографічних перетворень та сліпого електронного цифрового підпису / В.Г. Красиленко, Д.В. Нікітович, Р.О. Яцковська, В.І. Яцковський // Системи обробки інформації: збірник наукових праць. – Х.: Харківський університет Повітряних Сил імені Івана Кожедуба, 2019. – Вип. 1 (156). – С. 92-100. – [Електронний ресурс]. – Режим доступу: https://doi.org/10.30748/soi.2019.156.12

16. Красиленко В.Г. Моделювання протоколів узгодження секретного матричного ключа для криптографічних перетворень та систем матричного типу / В.Г. Красиленко, Д.В. Нікітович // Системи обробки інформації. – 2017. – Вип. 3 (149). – С 151-157.

17. Красиленко В.Г. Моделювання багатокрокових та багатоступеневих протоколів узгодження секретних матричних ключів / В.Г. Красиленко, Д.В. Нікітович // Комп`ютерно-інтегровані технології: освіта, наука, виробництво: науковий журнал. – Луцьк: ЛНТУ, 2017. – Вип. 26. – С 111-120. - Режим доступу: http://ki.lutsk-ntu.com.ua/node/134/section/27 .

18. Красиленко В.Г. Моделювання процесів генерування матричних ключів / В.Г. Красиленко, Д.В. Нікітович // «Інформаційні технології в освіті, науці і техніці» (ІТОНТ-2018): Збірник тез доповідей IV Міжнародної науково-практичної конференції, 17-18 травня 2018 року.–Черкаси: ЧДТУ, 2018. – С. 32-35. Режим доступу: https://chdtu.edu.ua/itont-2018/materiali-konferentsiji

19. Красиленко В.Г. Моделювання методів генерування потоків матричних перестановок значної розмірності для криптографічних перетворень зображень // В.Г. Красиленко, Д.В. Нікітович // Тези доповідей II Всеукраїнської науково-технічної конференції Комп'ютерні технології: інновації, проблеми, рішення (14 – 15 листопада 2019 р.) . – Житомир: Житомирська політехніка, 2019. – С. 67-77. – Режим доступу: https://conf.ztu.edu.ua/wp-content/uploads/2019/12/67-1.pdf